



TITLE:

多値論理関数とそのカスケード合成 (多値論理およびその応用研究会報告集)

AUTHOR(S):

原尾, 政輝; 鈴木, 淳之; 野口, 正一; 大泉, 充郎

CITATION:

原尾, 政輝 ...[et al]. 多値論理関数とそのカスケード合成 (多値論理およびその応用研究会報告集). 数理解析研究所講究録 1970, 81: 126-165

ISSUE DATE:

1970-03

URL:

<http://hdl.handle.net/2433/108027>

RIGHT:

多値論理関数とそのカスケード合成

原尾 政輝 鈴木 淳之 野口 正一 大泉 充郎

(東北大学電気通信研究所)

まえがき. 最近多値論理回路網, 特に三値論理回路網の研究が重要視されている。しかし多値論理代数に関しては若干の考察がなされているが, その複雑さのために詳しい性質はあまり知られていない。従ってこれらの回路網での合成を考える場合それに適した論理系を導くことが必要である。一般にこれらの論理系は基本演算の定義によって種々の形をとりうるが, ここでは二値論理の環和展開系の多値への拡張としての多値論理関数も定義する。この代数系はよく知られている環の構造をもち, 作用素をもつベクトル空間としてのところにより, 統一的に論じることが出来る。又このように定義された任意の論理関数のカスケードによる合成の問題はアフィン変換の概念を用いれば自由入力端子数 1 の基本素子(セル)の直列接続によって常に合成可能であるという結論を得る。最後に具体的回路網合成法を示し, 特に三値関数に対しては具体的合成例を与え, 回路網合成に必要な基本素子は一種で充分であることを示す。

1. 多値論理関数の性質

1.1. 多値論理関数の定義

真理値定数の集合を $Z_r = \{0, 1, \dots, r-1\}$ とし、その間に有理整数環の剰余環と同型の演算すなわち " $\text{mod } r$ " での加法 " \oplus " 乗法 " \cdot " を定義する。これを表1.1, 表1.2 に示す。

\oplus	0	1	2	3	...	$r-1$
0	0	1	2	3	...	$r-1$
1	1	2	3	4	...	0
2	2	3	4	5	...	1
3	3	4	5	6	...	2
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
$r-1$	$r-1$	0	1	2	...	$r-2$

(表1.1)

\cdot	0	1	2	3	...	$r-1$
0	0	0	0	0	...	0
1	0	1	2	3	...	$r-1$
2	0	2	4	6	...	$r-2$
3	0	3	6	9	...	$r-3$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
$r-1$	0	$r-1$	$r-2$	$r-3$...	1

(表1.2)

定理 1. 演算 $\langle \oplus, \cdot \rangle$ は可換分配系であり次の関係が成り

立つ; (1) 結合律 $x \oplus (y \oplus z) = (x \oplus y) \oplus z, \quad x(y \cdot z) = (x \cdot y) \cdot z$

(2) 交換律 $x \oplus y = y \oplus x, \quad x \cdot y = y \cdot x$

(3) 分配律 $x \cdot (y \oplus z) = (y \oplus z) \cdot x = x \cdot y \oplus x \cdot z$

(4) 零元・単位元の存在 $0 \oplus x = x, \quad 1 \cdot x = x$

又:これらの分配系が体になるための必要十分条件は r が素数なることに注意しよう。

今 n を与えられた性質の正の整数とするとき、次のような

$$\text{デカルト積} \quad \mathbb{Z}_r^n = \mathbb{Z}_r \times \mathbb{Z}_r \times \cdots \times \mathbb{Z}_r \quad \text{--- (1.1)}$$

を考えよう。 \mathbb{Z}_r^n の元は r^n 個の順序づけられた元で

$$(x_1, x_2, \dots, x_n) \quad \text{--- (1.2)}$$

とかける。又 \mathbb{Z}_r^n は ユークリッド空間 R^n の部分空間で (1.2) 式で表わされる成分を点とよぶ。 \mathbb{Z}_r^n を n -cube と書くこともある。これを $r=3$ について図 1.1 に示す。

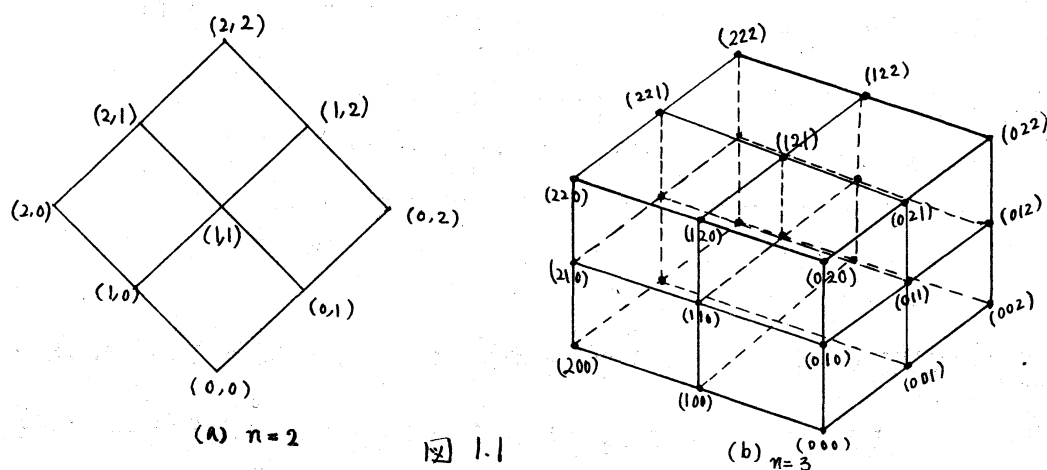


図 1.1

ここで n 変数関数 $f(x_1, x_2, \dots, x_n)$ を写像

$$f: \mathbb{Z}_r^n \rightarrow \mathbb{Z}_r \quad \text{--- (1.3)}$$

と定義する。特に n -cube のすべての点に対して 1 を与える単位関数を 1, 0 を与える零関数を 0 で表わす。写像 f の集合を \mathcal{F}_n とすれば、 \mathcal{F}_n の基数は r^{r^n} である。

f, g を \mathcal{F}_n の任意の二元とするとき、これらの演算を

$$f \oplus g = h \Leftrightarrow f(x_1, \dots, x_n) \oplus g(x_1, \dots, x_n) = h(x_1, \dots, x_n)$$

$$f \cdot g = h \Leftrightarrow f(x_1, \dots, x_n) \cdot g(x_1, \dots, x_n) = h(x_1, \dots, x_n)$$

と定義するとき、 \mathcal{F}_n の部分集合 $F = \{f\}$ の組み合わせで任意の \mathcal{F}_n の元が導出可能であるとき、この論理系 $\langle F, \oplus, \cdot \rangle$ は定備系をなすといふ。ここではフル環の多値への拡張としての定備系を導く。

今一変数関数を x とし $\overbrace{x \cdot x \cdots x}^i = x^i$, $\overbrace{x \oplus x \oplus \cdots \oplus x}^i = i x$ と書くことにする。この定義によって各 R の真理値表表示は表13, 表14に表わされるように、各成分毎の積と和によって実現される。従って論理系 $\langle \oplus, \cdot \rangle$ の全ての元は単位関数1と一変数関数の中 $\{x, x^2, \dots, x^{r-1}\}$ の一次結合で表わされるが、これが定備である R の条件を求めてみる。

x	x^2	x^3	\dots	x^{r-1}	1
0	0	0		0	1
1	1	1		1	1
2	2^2	2^3		2^{r-1}	1
3	3^2	3^3		3^{r-1}	1
\vdots	\vdots	\vdots		\vdots	\vdots
$r-1$	$(r-1)^2$	$(r-1)^3$		$(r-1)^{r-1}$	1

(表13)

x	$2x$	$3x$	\dots	$(r-1)x$	$\alpha 1$
0	0	0		0	α
1	2	3		$r-1$	α
2	4	6		$r-2$	α
3	6	9		$r-3$	α
\vdots	\vdots	\vdots		\vdots	\vdots
$r-1$	$r-2$	$r-3$		1	α

(表1.4)

まず表 1.5 に示されるような関数

$$J_i(x) = \begin{cases} 1 & \text{if } x = i \\ 0 & \text{if } x \neq i \end{cases}$$

を定義し、基底関数とよぶ。

明らかにこの基底関数が導出可能なことが任意の一変数関数が合成可能なための必要十分条件である。

x	$J_0(x)$	$J_1(x)$	\dots	$J_{r-1}(x)$
0	1	0		0
1	0	1		0
2	0	0	\dots	0
\vdots	\vdots	\vdots		\vdots
$r-1$	0	0		1

(表1.5)

関数空間 \mathcal{F}_n から \mathbb{Z}_r の元を成分とする r^n -タプル の集合

\mathcal{Q}_n への写像 χ を

$$\forall p \in \mathbb{Z}_r^n, \quad f: p = (x_1, x_2, \dots, x_n) \rightarrow i_p, \quad i_p \in \mathbb{Z}_r$$

$$\Rightarrow \chi(f) = (i_0, i_1, \dots, i_p, \dots, i_{r^n-1}) \quad \text{--- (1.4)}$$

とすれば χ は同型である。又 $\chi^{-1} = \lambda$ とおく。

これによって

$$\forall f, g \in \mathcal{F}_n, \quad \chi \cdot f(x_1, \dots, x_n) = (i_0, i_1, \dots, i_{r^n-1})$$

$$\psi \cdot g(x_1, \dots, x_n) = (j_0, j_1, \dots, j_{r^n-1})$$

$$\Rightarrow \chi \left(f(x_1, \dots, x_n) \oplus g(x_1, \dots, x_n) \right) = (i_0 \oplus j_0, i_1 \oplus j_1, \dots, i_{r^n-1} \oplus j_{r^n-1})$$

$$\chi \left(f(x_1, \dots, x_n) \odot g(x_1, \dots, x_n) \right) = (i_0 \cdot j_0, i_1 \cdot j_1, \dots, i_{r^n-1} \cdot j_{r^n-1})$$

と成分毎の加法、乗法が成立し、 \mathbb{Z}_r -加群とみなすことができる。一変数関数はそれらの部分空間をつくり、各変数に関する基底関数の積を表1.6に示す。今 $X = \{x_1, x_2, \dots, x_n\}$ とおくと

$x_n \dots x_2 x_1$	$J_0(x_1) J_0(x_2) \dots J_0(x_n), J_1(x_1) J_0(x_2) \dots J_0(x_n), \dots, J_{r-1}(x_1) J_{r-1}(x_2) \dots J_{r-1}(x_n)$
0 ... 0 0	1
0 ... 0 1	0
0 ... 0 \vdots	\vdots
0 ... 0 $r-1$	0
0 ... 1 0	0
0 ... 1 1	0
0 ... 1 \vdots	\vdots
0 ... 1 $r-1$	0
\vdots	\vdots
$r-1 \dots r-1 0$	0
$r-1 \dots r-1 1$	0
$\vdots \dots \vdots \vdots$	\vdots
$r-1 \dots r-1 r-1$	1

(表6)

定理 2. 論理系 $\langle X, \oplus, \cdot, 1 \rangle$ が完備系をなすための必要十分条件は各変数に対する基底関数が $\{1, x, \dots, x^{r-1}\}$ の一次結合として一意的に求まることである。

(証明) $J_i(x)$ が一意的に求まれば表 1.6 に示されるように \mathcal{Q}_n の表現では一成分に真理値 1 をもつ関数である。これは最小項に相当し $m_i(x_1, \dots, x_n)$ と記し最小関数と定義する。ここで

$$\begin{cases} x \cdot m_0(x_1, \dots, x_n) = \chi(J_0(x_1) \cdots J_0(x_n)) = (1, 0, \dots, 0) \\ x \cdot m_1(x_1, \dots, x_n) = \chi(J_1(x_1) \cdots J_0(x_n)) = (0, 1, \dots, 0) \\ \vdots \\ x \cdot m_{r^n-1}(x_1, \dots, x_n) = \chi(J_{r-1}(x_1) \cdots J_{r-1}(x_n)) = (0, 0, \dots, 1) \end{cases} \quad (1.5)$$

と置けば \mathcal{F}_n の任意の元 f はこれらの一次結合として

$$f = \sum_{i=0}^{r^n-1} d_i \cdot m_i(x_1, \dots, x_n), \quad 0 \leq d_i \leq (r-1) \quad (1.6)$$

と一意に表わせる。逆に完備性の定義より、これが完備ならば一変数関数が求まらねばならぬから基底関数が求まる必要がある。又変数は r 個 $\{1, x, \dots, x^{r-1}\}$, 基底関数も r 個であるから一意に求まらねばならぬ。(証明終)

今後集合 \mathcal{F}_n と環 \mathcal{Q}_n は同型対応をなすから \mathcal{F}_n の元と \mathcal{Q}_n の元とを同一視する。

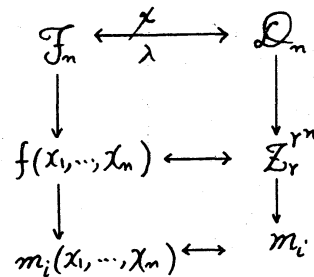


図 1.2

定理 3 論理系 $\langle X, \oplus, \cdot, 1 \rangle$ が完備であるための必要+

分条件は r が素数なることである。

(証明) 定理 2 より, 基底関数 $J_i(x)$ が一意的に求まることを示せばよい。これは $a_i \in \mathbb{Z}_r$ とするとき, 次の連立一次方程式が唯一の解を持つことと同値である。

$$\left\{ \begin{array}{l} a_0 \cdot 1 \oplus 0 \oplus \cdots \oplus 0 = \beta_0 \\ a_0 \cdot 1 \oplus a_1 \oplus \cdots \oplus a_{r-1} = \beta_1 \\ a_0 \cdot 1 \oplus a_1 \cdot 2 \oplus \cdots \oplus a_{r-1} \cdot 2^{r-1} = \beta_2 \\ \vdots \\ a_0 \cdot 1 \oplus a_1 \cdot (r-1) \oplus \cdots \oplus a_{r-1} \cdot (r-1)^{r-1} = \beta_{r-1} \end{array} \right. \quad (1.7)$$

行列式 A を求めると

$$A = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (r-1) & (r-1)^2 & \cdots & (r-1)^{r-1} \end{vmatrix} = 2 \cdot 3 \cdots (r-1) \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-2} \\ 1 & 3 & 3^2 & \cdots & 3^{r-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (r-1) & (r-1)^2 & \cdots & (r-1)^{r-2} \end{vmatrix} = k \cdot A_{r-1}$$

$$A_{r-1} = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (r-1) & (r-1)^2 & \cdots & (r-1)^{r-2} \end{vmatrix} = \begin{vmatrix} 1 & 2 & \cdots & 2^{r-4} & 2^{r-3} \\ 2 & 2 \cdot 3^{r-2} & \cdots & 2 \cdot 3^{r-4} & 2 \cdot 3^{r-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (r-2) & (r-2)(r-1) & \cdots & (r-2)(r-1)^{r-4} & (r-2)(r-1)^{r-3} \end{vmatrix} = 2 \cdot 3 \cdots (r-1) \begin{vmatrix} 1 & 2 & \cdots & 2^{r-4} & 2^{r-3} \\ 1 & 3 & \cdots & 3^{r-4} & 3^{r-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & (r-1) & \cdots & (r-1)^{r-4} & (r-1)^{r-3} \end{vmatrix}$$

$$= k_1 \begin{vmatrix} 1 & 1 & 2 & \cdots & 2^{r-5} & 2^{r-4} \\ 1 & 2 & 2 \cdot 3 & \cdots & 2 \cdot 3^{r-5} & 2 \cdot 3^{r-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & (r-2) & (r-2)(r-1) & \cdots & (r-2)(r-1)^{r-5} & (r-2)(r-1)^{r-4} \end{vmatrix} = k_1 \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-5} & 2^{r-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & (r-2) & (r-2)^2 & \cdots & (r-2)^{r-5} & (r-2)^{r-4} \end{vmatrix} = k_1 \cdot A_{r-2}$$

同様にして $A = k \cdot k_1 \cdot \dots \cdot k_{r-3} \cdot A_2$ をえる。

但し $k = 2 \cdot 3 \cdot \dots \cdot (r-1)$, $k_i = 2 \cdot 3 \cdot \dots \cdot (r-i-1)$

$$A_2 = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = 1$$

ゆえに $A = 2^{r-2} \cdot 3^{r-2} \cdot \dots \cdot (r-2)^2 \cdot (r-1)$ — (1.8)

(i) A は r の素数ならば $A \not\equiv 0 \pmod{r}$ を満す

(ii) $A \not\equiv 0 \pmod{r}$ と仮定する。

(a) $r = 3$ なら $A = 2 \not\equiv 0 \pmod{3}$ より条件を満す。

(b) $r = 4$ なら $A \equiv 0 \pmod{4}$ より条件を満す。

(c) $r \geq 5$ と仮定する。この時証明のためにまず次の補題を示す。

補題 1. r を $r \geq 5$ なる任意の整数とすれば、 $2 \leq x \leq r-2$ に対して $(r-x)^x > r$ が成立する。

(証明) $f(x) = (r-x)^x - r$ とおく。

$$\frac{df}{dx} = \frac{d}{dx} \left(e^{x \log_e(r-x)} - r \right) = \left(\log_e(r-x) + \frac{-x}{r-x} \right) (r-x)^x$$

仮定より $(r-x)^x > 0$

(a) $g(x) = \log(r-x) - \frac{x}{r-x}$ とおけば

$$\frac{dg(x)}{dx} = \frac{x-2r}{(r-x)^2} < 0 \quad (2 \leq x \leq r-2) \quad \text{より } g(x) \text{ は単調減少}$$

$$\text{かつ } g(2) = \log(r-2) - \frac{2}{r-2} > 0, \quad g(r-2) = \log 2 + \frac{2-r}{2} < 0$$

より f は Fig. 1.3 のようになる。

$$(b) \quad f(2) = (r-2)^2 - r = r^2 - 5r + 4, \quad \text{かつ} \quad \frac{df(2)}{dr} = 2r - 5 > 0$$

より r に関して単調増加, かつ $f(2)|_{r=4} = 0$. $f(2)|_{r=5} = 4$,

$$(c) \quad f(r-2) = 2^{r-2} - r, \quad \text{かつ} \quad \frac{df(r-2)}{dr} = (\log 2) \cdot 2^{r-2} > 0$$

より r に関して単調増加, かつ $f(r-2)|_{r=4} = 0$ $f(r-2)|_{r=5} = 3$

即ち $r \geq 5$ であれば $f > 0$ ゆえに $(r-x)^x > r$

(証明終)

従って補題 1 より

$$A = 2^{r-2} \cdot 3^{r-3} \cdots (r-2)^2 (r-1) \not\equiv 0 \pmod{r}$$

で $r = 2^{\varepsilon_2} \cdot 3^{\varepsilon_3} \cdots (r-1)^{\varepsilon_{r-1}}$ と分解されたとすると, 各因子 i^{ε_i} は A の因子に含まれている。故に指数 $\varepsilon_2, \dots, \varepsilon_{r-2}$ は全て零でなければならない。即ち r は素数でなければならない。

(証明終)

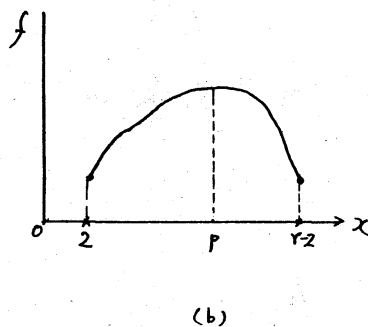
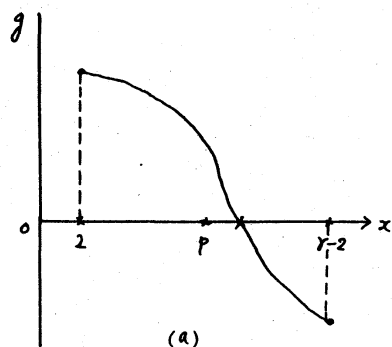


Fig. 1.3

1.2 多値論理関数の表現

一般には: : で定義した演算以外に更に独立な単項演算も定義すれば, \mathcal{Y} が素数以外でも完備系にすることが可能である。しかし実際回路網を合成する場合には演算が簡単は程, 構成素子が少なくてすみ能率的である。又: : に定義した関数の構造はカスケード合成に適しており, 以後 \mathcal{Y} を素数に限って: の関数の性質と合成法を述べてゆく。

補題2. (ウルソンの定理) \mathcal{Y} を素数とすれば, $(\mathcal{Y}-1)! \equiv -1 (\mathcal{Y})$

(証明) $GF(\mathcal{Y}^n)$ の 0 と異なるすべての要素を a_1, a_2, \dots, a_h とすると

$$x^h - 1 = \prod_{i=1}^h (x - a_i)$$

が成り立つから $a_1 \cdot a_2 \cdot \dots \cdot a_h = -1$

特に $n=1$ とすると \mathcal{Y} が素数だから $1, 2, \dots, (\mathcal{Y}-1)$ が $GF(\mathcal{Y})$ のえで $(\mathcal{Y}-1)! \equiv -1 \pmod{\mathcal{Y}}$ (証明終)

定理4. 基底関数 $J_i(x)$ は次のように書ける:

$$J_i(x) = (\mathcal{Y}-1) \cdot x \cdot (x \oplus 1) \cdots (x \oplus (\mathcal{Y}-i-1)) \cdot (x \oplus (\mathcal{Y}-i+1)) \cdots (x \oplus (\mathcal{Y}-1)) \quad \text{--- (1.9)}$$

$$\text{又 } J_i(x) \cdot J_j(x) = \begin{cases} J_i(x) & \text{if } i=j \\ 0 & \text{if } i \neq j \end{cases} \quad \text{--- (1.10)}$$

(証明) $x = i'$ とおけば (1.9) 式右边は $(\mathcal{Y}-1) \cdot i' \cdot (i'+1) \cdots (\mathcal{Y}-1) \cdot$

$$\begin{aligned} 1 \cdot 2 \cdots (i'-1) &= 1 \cdot 2 \cdots (i'-1) \cdot i' \cdot (i'+1) \cdots (\mathcal{Y}-2) (\mathcal{Y}-1)^2 \\ &= (\mathcal{Y}-1) \cdot (\mathcal{Y}-1)! \end{aligned}$$

補題2より $(r-1)! = (r-1)$, $\therefore (r-1)(r-1)! \equiv 1 \pmod{r}$

$J_i(j)$ ($i \neq j$) なら明らかに $J_i(j) = 0$ 故に成立.

$J_i^2(x)$ は $x = i$ のとき $J_i(i) = 1$ 故から $J_i^2(x) = 1$ その他以外では0故から $J_i^2(x) = J_i(x)$, 又 $J_i(x) \cdot J_j(x)$ は同時に真理値1をとることはないので $J_i(x) \cdot J_j(x) = 0$ (証明終)

関数空間 \mathcal{F}_n 空間に成り立つ性質を調べてみよう.

定理5. \mathcal{F}_n の元の間には次の演算が成立する.

$$(1) f^r = f^{tr} = f, \quad rX = r \cdot X = 0 \quad (r=1, 2, \dots)$$

$$(2) (if)(jg) = (ij)fg, \quad if \oplus jf = (i \oplus j)f$$

$$(3) f \oplus g = g \oplus f, \quad f \cdot g = g \cdot f$$

$$(4) f \cdot (g \cdot h) = (f \cdot g) \cdot h, \quad f \oplus (g \oplus h) = (f \oplus g) \oplus h$$

$$(5) f \cdot (g \oplus h) = (g \oplus h) \cdot f = f \cdot g \oplus f \cdot h$$

(証明) (1) r が素数であるから Fermat の定理より $a \neq 0$ なる任意の数に対して $a^{r-1} \equiv 1 \pmod{r}$ が成立する.

$$f = (a_1, a_2, \dots, a_{r^n}), \quad a_i \in \mathbb{Z}_r$$

$$\text{とおくと } f^{r-1} = (a_1^{r-1}, a_2^{r-1}, \dots, a_{r^n}^{r-1}) = (1, 1, \dots, 1) = 1$$

$$\text{故に } f^r = f, \text{ 同様にこれをくり返せば } f^{tr} = f.$$

$$\text{又加法に対しては } rf = (ra_1, ra_2, \dots, ra_{r^n}) = (0, 0, \dots, 0) = 0$$

(2) 作用素 \mathbb{Z}_r は可換体であるから

$$f = (a_1, a_2, \dots, a_{r^n}), \quad g = (b_1, b_2, \dots, b_{r^n})$$

$$\Rightarrow (if)(jg) = (ia_1, ia_2, \dots, ia_{r^n}) \cdot (jb_1, jb_2, \dots, jb_{r^n})$$

$$\begin{aligned}
&= ((i a_1)(j b_1), (i a_2)(j b_2), \dots, (i a_{r^n})(j b_{r^n})) \\
&= (i j (a_1 b_1), i j (a_2 b_2), \dots, i j (a_{r^n} b_{r^n})) \\
&= (i j f)(f, g)
\end{aligned}$$

(3), (4) も同様にして求める。

$$\begin{aligned}
(5) \quad f \cdot (g \oplus h) &= (a_1, a_2, \dots, a_{r^n}) \cdot (b_1 \oplus c_1, b_2 \oplus c_2, \dots, b_{r^n} \oplus c_{r^n}) \\
&= (a_1(b_1 \oplus c_1), a_2(b_2 \oplus c_2), \dots, a_{r^n}(b_{r^n} \oplus c_{r^n})) \\
&= ((b_1 \oplus c_1) a_1, (b_2 \oplus c_2) a_2, \dots, (b_{r^n} \oplus c_{r^n}) a_{r^n}) = (g \oplus h) \cdot f \\
&= (a_1 b_1 \oplus a_1 c_1, a_2 b_2 \oplus a_2 c_2, \dots, a_{r^n} b_{r^n} \oplus a_{r^n} c_{r^n}) = f g \oplus f h
\end{aligned}$$

(証明終)

二値の場合、ブール環は全ての元が $f^2 = f$ なる中等元であるという定義であった。この一般化として (1) に示されるように多値環 \mathcal{Q}_n を $f^r = f$ なる元よりなる可換環として定義することができる。又任意の与えられた多値論理関数 f の点 m_j に対する真理値を t_j とすれば、関数 f は次のように最小関数の一次結合として展開される。

定理 6. 任意の関数は加法展開公式を用いて次のように求まる。

$$f(x_1, \dots, x_n) = J_0(x_1) \cdot f(0, x_2, \dots, x_n) \oplus J_1(x_1) \cdot f(1, x_2, \dots, x_n)$$

$$\oplus \dots \oplus J_{r-1}(x_1) \cdot f(r-1, x_2, \dots, x_n) \quad \text{—— (1.11)}$$

$$= \sum_{i=0}^{r-1} x_i^{m_i} m_i(x_1, \dots, x_n) \quad \text{—— (1.12)}$$

(証明) (1.11) 式において 左辺 = $f(x_1, x_2, \dots, x_n)$ とすると右辺は

$$J_i(i) \cdot f(i, x_2, \dots, x_n) = f(i, x_2, \dots, x_n)$$

故に公式が成立する。これを繰り返して使用すると、 $m_i(x_1, \dots, x_n)$
 $= J_{i_1}(x_1) \cdot J_{i_2}(x_2) \cdot \dots \cdot J_{i_n}(x_n)$ は i 成分 k のみ 1 をもつ項となるから、それに真理値 x_i を与えれば

$$f(x_1, \dots, x_n) = \sum_{i=0}^{r^n} x_i m_i(x_1, \dots, x_n)$$

が成り立つ。

(証明終)

$J_0(x_1) \oplus J_1(x_1) \oplus \dots \oplus J_{r-1}(x_1) = 1$ を用いて (1.11) 式を変形すれば次の乗法展開公式が得られる。

系 1. 乗法展開公式 $f(i, x_2, \dots, x_n) = f(i)$ とおくと

$$\begin{aligned} f(x_1, \dots, x_n) &= (f(0) \oplus J_1 \oplus \dots \oplus J_{r-1}) (f(1) \oplus J_0 \oplus J_2 \oplus \dots \oplus J_{r-1}) \\ &\quad \dots (f(r-1) \oplus J_0 \oplus \dots \oplus J_{r-2}) \\ &= ((f(0)-1)J_0 \oplus 1) \cdot ((f(1)-1)J_1 \oplus 1) \cdot \dots \cdot ((f(r-1)-1)J_{r-1} \oplus 1) \quad (1.13) \end{aligned}$$

例題 1. 三値論理関数の基底関数を求め、次に与えられた真理値表表示を展開せよ。

x	y	f
0	0	1
0	1	2
0	2	1
1	0	0
1	1	2
1	2	0
2	0	1
2	1	0
2	2	2

x	x^2	$J_0(x)$	$J_1(x)$	$J_2(x)$
0	0	1	0	0
1	1	0	1	0
2	1	0	0	1

$$J_0(x) = 1 \oplus 2x^2$$

$$J_1(x) = 2x \oplus 2x^2$$

$$J_2(x) = x \oplus 2x^2$$

$$\begin{aligned}
f &= J_0(y) \cdot J_0(x) \oplus 2J_1(y) \cdot J_0(x) \oplus J_2(y) \cdot J_0(x) \\
&\oplus 0 \cdot J_0(y) \cdot J_1(x) \oplus 2J_1(y) \cdot J_1(x) \oplus 0 \cdot J_2(y) \cdot J_1(x) \\
&\oplus J_0(y) \cdot J_2(x) \oplus 0 \cdot J_1(y) \cdot J_2(x) \oplus 2 \cdot J_2(y) \cdot J_2(x) \\
&= (1 \oplus 2x^2)(1 \oplus 2y^2) \oplus 2(2y^2 \oplus 2y)(2x^2 \oplus 1) \oplus (2y^2 \oplus y)(2x^2 \oplus 1) \\
&\oplus 2(2y^2 \oplus 2y)(2x^2 \oplus 2x) \oplus (2y^2 \oplus 1)(2x^2 \oplus x) \oplus 2(2x^2 \oplus x)(2y^2 \oplus y) \\
&= x^2 \oplus x^2y \oplus xy \oplus 2xy^2 \oplus x \oplus 2y^2 \oplus 2y \oplus 1
\end{aligned}$$

1.3. 多値論理関数の代数的構造

関数空間 \mathcal{Q}_n の構造を調べてみる。前節で述べたように多値環 \mathcal{Q}_n は r^n タップルの成分毎の乗法と加法に対して環をなし、 $f^r = f$ を満す可換環であった。又係数体 Z_r を作用素とする多値環とみる：とができる。これは

$$\begin{aligned}
\forall a \in Z_r, \quad f, g \in \mathcal{Q}_n \\
a(f \cdot g) &= (af)g = f(a \cdot g)
\end{aligned}$$

が成り立つことが容易に示される。

更に：

これらの基底は m_i ($0 \leq i \leq r^n - 1$) であった。

\mathcal{Q}_n の部分集合を B とするとき

$$(i) \quad f, g \in B \Rightarrow f - g \in B$$

$$(ii) \quad f \in B, g \in \mathcal{Q}_n \Rightarrow f \cdot g \in B \quad (\text{又は } g \cdot f \in B)$$

の条件を満すとき左(右) ideal とよばれる。ここでは可換環であるから両側 ideal である。

定理 7 最小関数の集合を $P_n = \{m_0, m_1, \dots, m_{r_n}\}$

P_n の部分集合を $\Lambda = \{m_{i_1}, \dots, m_{i_k}\}$ とする。このとき

Λ の元の一次結合で生成される関数 Λ^* は \mathcal{Q}_n の ideal を作る。

(証明) (i) $\forall f, g \in \Lambda^*, f = \sum_{m_{ij} \in \Lambda} c_j m_{ij}, g = \sum_{m_{ij} \in \Lambda} d_i m_{ij}$

ゆえに $f - g = \sum_{m_{ij} \in \Lambda} (c_j - d_j) m_{ij} \in \Lambda^*$

(ii) $\forall f \in \Lambda^*, \forall g \in \mathcal{Q}_n, g = \sum_{m_{ij} \in P_n} e_j m_{ij}$

ゆえに $f \cdot g = \left(\sum_{m_{ij} \in \Lambda} c_j m_{ij} \right) \left(\sum_{m_{ij} \in P_n} e_j m_{ij} \right)$

$$= \sum_{m_{ij} \in \Lambda} c_j e_j m_{ij} \in \Lambda^* \left(\because m_i \cdot m_j = \begin{cases} 0 & \text{if } i \neq j \\ m_i & \text{if } i = j \end{cases} \right)$$

(証明終)

特に一個の最小関数の結合のみよりなる部分集合も明らかに ideal を作り、これを単項 ideal とよぶ。

定理 8 各最小関数 m_i によって生成される単項 ideal を

\mathcal{O}_i とおくと、 $\mathcal{O}_i = \mathcal{Q}_n \cdot m_i$ で

$$\mathcal{Q}_n = \mathcal{O}_0 \oplus \mathcal{O}_1 \oplus \dots \oplus \mathcal{O}_{r_n-1}$$

と一意的に表わされる。

(証明) 単位元 $1 = m_0 \oplus m_1 \oplus \dots \oplus m_{r_n-1}$ と分解され

$m_i \cdot m_j = 0$ (if $i \neq j$), $m_i^2 = m_i$ より \mathcal{Q}_n は m_i より生成される

ideal の直和であることがわかる。又単項 ideal \mathcal{O}_i は生成元の

のみで生成される関数であるから、 $\mathcal{O}_i = \mathcal{Q}_n \cdot m_i$. (証明終)

環の ideal の集合や環の部分環の集合はその包含関係の下に束をなす。この多値環の束構造を調べてみる。

環 \mathbb{Q}_m の任意の 2 元 $a = (i_0, i_1, \dots, i_{r-1})$, $b = (j_0, j_1, \dots, j_{r-1})$ に対し

$$a \geq b \iff \forall p, i_p \geq j_p$$

と関係 \geq を定義する。

補題 3 関係 \geq は順序関係で, (\mathbb{Q}_m, \geq) は半順序集合をなし、更に完備束である。

(証明) \mathbb{Q}_m は全順序集合だから (i) $a \geq a$, (ii) $a \leq b, b \leq c \Rightarrow a \leq c$
 (iii) $a \geq b, a \leq b \Rightarrow a = b$ が成り立つことは明らか。^{故に} 半順序集合であって

$$a \cup b = (i_0 \cup j_0, i_1 \cup j_1, \dots, i_{r-1} \cup j_{r-1})$$

$$a \cap b = (i_0 \cap j_0, i_1 \cap j_1, \dots, i_{r-1} \cap j_{r-1})$$

$$\text{但し } i \cup j = \max(i, j), \quad i \cap j = \min(i, j)$$

とおくと 上限 $\sup \{a, b\} = a \cup b$, 下限 $\inf \{a, b\} = a \cap b$ が存在するから束をなし、有限束であるから完備束である。

(証明終)

$L_m = \langle \mathbb{Q}_m, \cup, \cap \rangle$ とおくと L_m は \cup, \cap について

(1) 中等律 (2) 結合律 (3) 交換律 (4) 吸収律 を満たす可換半群をつくっている。

定理 9 束 L_m は最大元、最小元を持つ分配束である。

(証明) $I = (r-1, r-1, \dots, r-1)$, $0 = (0, 0, \dots, 0)$ とおけば任意の L_m の元に対して $0 \leq f \leq I$ よりそれぞれ最大

元と最小元である。分配律 $f \cap (g \cup h) = (f \cap g) \cup (f \cap h)$

$f \cup (g \cap h) = (f \cup g) \cap (f \cup h)$ が成り立つことは Σ_r が全順序集合

$$\text{だから } f_i \cap (g_i \cap h_i) = \begin{cases} f_i \cap g_i & \text{if } g_i \leq h_i \\ f_i \cap h_i & \text{if } g_i \not\leq h_i \end{cases}, (f_i \cap g_i) \cup (f_i \cap h_i) = \begin{cases} f_i \cap g_i & \text{if } g_i \leq h_i \\ f_i \cap h_i & \text{if } g_i \not\leq h_i \end{cases}$$

より示される。

(証明終)

フーリエには (i) $f \cup \bar{f} = 1$ (ii) $f \cap \bar{f} = 0$ の存在が必要であるが、 L_n はこの条件を満たさない。この相補律の代りに次のような演算を L_n に定義する。

$$(1) \tilde{f} = 1 \oplus f \quad (\oplus \text{ は } \oplus \text{ に対する逆元}) \quad (2) f^{\sim} = f \oplus 1$$

すると $L^* = \langle \cup, \cap, \sim, \neg \rangle$ は位相系をなし Post 代数とよばれる。今 r を事象とすれば \mathcal{F}_n と L^* は次の対応をなす (3他)

$$x \cup y = x^2 y^2 \oplus x^2 y \oplus x y^2 \oplus 2xy \oplus x \oplus y$$

$$x \cap y = 2x^2 y^2 \oplus 2x^2 y \oplus 2x y^2 \oplus xy$$

$$\tilde{x} = 2 \oplus 2x, \quad x^{\sim} = 1 \oplus x, \quad \hat{x} = 1 \oplus 2x, \quad \bar{x} = 2 \oplus x \text{ etc.}$$

\mathcal{Q}_n の順序関係 \succeq に対して

$$(1) a \succeq b \Rightarrow b = a \text{ 又は } b = 0$$

が成り立つとき \mathcal{Q}_n の元 a は atom であることが示される。 \mathcal{Q}_n の atom は基底 m_i である。これもフーリエ環の拡張概念である。

2. 多段論理回路網による多値論理関数の合成

2.1 多段論理回路網の表現

取り扱う回路は純組合せ的であるとする。この回路網の基本素子をセルとよび、数種のセルのカスケードよりなる回路を多段論理回路。特に一種のセルのカスケードよりなる回路を反復論理回路とよぶ。(Fig. 1).

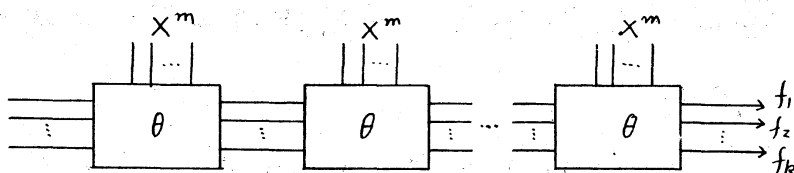


図 2.1

なお r 端子入力を自由変数, y 入力を接続変数とよび, それぞれ r 値で r は素数とする。又 r 端子 m , 接続端子 k のセルを (m, k) -セルと略記する。すなわち (m, k) -セルの接続変数を

$$(y_1, y_2, \dots, y_k) \mapsto y_k + r \cdot y_{k-1} + \dots + r^{k-1} y_1 \quad (2.1)$$

と対応させ, この整数の集合 $N = \{0, 1, \dots, r^k - 1\}$ を状態集合とよぶ。集合 N の上の変換を $\mathcal{T}_N = \{t \mid N \rightarrow N\}$ とすればセル θ は入力の制御の下での写像

$$\theta : \mathbb{Z}_r^m \rightarrow \mathcal{T}_N \quad (2.2)$$

とみはすことができる。特に $r=2$ では θ の値域として可換群 $H \subset \mathcal{T}_N$ をとる。すると多値関数 $f : \mathbb{Z}_r^n \rightarrow N$ の合成問題は変換回路網 $f : \mathbb{Z}_r^n \rightarrow H$ の合成問題に帰着される。又前章でのべたように関数 f は r^m 次元の N を成分とするベクトル空

間と同型だから、 f とそれらを同一視する。(今後変数の意味で Z_r の代りに X を用いる)

$$\text{今任意の群関数を } f_i : X^m \rightarrow H, \quad \text{--- (2.3)}$$

$$f_j : X^{m'} \rightarrow H$$

とすると、 r^m 次元空間の元として

$$f_i(X^m) = (h_0, h_1, \dots, h_{r^m-1}) \quad h_i \in H$$

$$f_j(X^{m'}) = (h'_0, h'_1, \dots, h'_{r^{m'}-1}) \quad h'_i \in H$$

と表わす。今 f_i と f_j のカスケードを $f_i \oplus f_j$ とすると

$$(f_i \oplus f_j)(X^m, X^{m'}) = f_i(X^m) \oplus f_j(X^{m'}) = (h_0 \oplus h'_0, h_1 \oplus h'_1, \dots, h_{r^m-1} \oplus h'_{r^{m'}-1})$$

と成分毎の和、即ちカスケードはベクトル空間の加法に対応する。

一般に回路網バセル $\theta_i : X^m \rightarrow H$ のカスケードで合成される時 m 変数で合成可能とよぶが、今後1変数での合成可能性について話を限ることとする。今1変数での変換回路網(群関数)の集合を \mathcal{H}_n と書く。 \mathcal{H}_n は群 H の元の間には乗法が定義できれば成分毎の積として環をつくる。 H を任意の可換群とすれば H の自己同型の全体は単位環をつくり、その作用素の意味での演算が乗法に対応する。ここでは自己準同型 $E(H)$ の加法 $E(H)^+$ と H を同一視する。

定理10 \mathcal{H}_n は H の自己準同型環 $E(H)$ が可換ならば $E(H)$

の上の階数 r^n の多項式環をなす。

(証明) 命題より $E(H)$ は単位可換環となるから

$$\forall f, g \in E(H), \quad \forall F, G \in \mathcal{H}_n$$

$$\begin{aligned}
h(F \cdot G) &= h((f_1, f_2, \dots, f_r) \cdot (g_1, g_2, \dots, g_r)) \\
&= (h(f_1 g_1), h(f_2 g_2), \dots, h(f_r g_r)) \\
&= ((h f_1) \cdot g_1, (h f_2) \cdot g_2, \dots, (h f_r) \cdot g_r) = (h \cdot F) \cdot G \\
&= (f_1(h g_1), f_2(h g_2), \dots, f_r(h g_r)) = F \cdot (h \cdot G)
\end{aligned}$$

(証明終)

このときベクトル基底の存在は H として位数 r^k の巡回群及び基本可換群 C_r^k をとれば次のように示される。

定理 11. 位数 r^k の巡回群を C_{r^k} とすれば、回路網 $f: X^n \rightarrow C_{r^k}$ の事象 \mathcal{H}_n は $\mathbb{Z}/(r^k)$ の上の階数 r^n の多え環と同型で、基底は一意的に定まる。

(証明) $E(C_{r^k})$ は $\mathbb{Z}/(r^k)$ と同型であるから、前定理より $\mathbb{Z}/(r^k)$ 上の階数 r^n の多え環として表わされ、基底は $\{1, x, x^2, \dots, x^{r-1}\}$ の一次結合として表現されねばならぬ。前章定理 3 の場合と同様に

$$A = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{r-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (r-1) & (r-1)^2 & \cdots & (r-1)^{r-1} \end{vmatrix} = 2^{r-2} \cdot 3^{r-3} \cdots (r-2)^2 (r-1) \not\equiv 0 \pmod{r}$$

であるから、 $A \not\equiv 0 \pmod{r^k}$ である。従って基底関数

$J_0(x), J_1(x), \dots, J_{r-1}(x)$ が一意的に求まる。又基底はこれらの積として一意的に定まる。 (証明終)

ベクトル基底を最小関数とよび, $m_i(x_1, x_2, \dots, x_n)$ とおくと \mathcal{H}_n の元はこれらの一次結合として一意的に次のように展開される;

$$f(x^n) = \sum_{i=0}^{r^n-1} d_i m_i(x_1, x_2, \dots, x_n) \quad \text{--- (2.4)}$$

$$m_i \cdot m_j = \begin{cases} 0 & \text{if } i \neq j \\ m_i & \text{if } i = j \end{cases}, \quad \sum_{i=0}^{r^n-1} m_i = 1 \quad \text{--- (2.5)}$$

$$d_i \in \mathbb{Z}/(r^k)$$

(2.5) 式より, $m_i(x_1, \dots, x_n)$ は atom で

$$\mathcal{H}_n = \mathcal{H}_n \cdot m_0 \oplus \mathcal{H}_n \cdot m_1 \oplus \dots \oplus \mathcal{H}_n \cdot m_{r^n-1} \quad \text{--- (2.6)}$$

と単項 ideal の直和に分解される。

同様に群 H として基本可換群 C_r^k をとると, $\mathbb{Z}/(r)$ 上の k 次元ベクトルと同型であるから次の結果を得る。

定理 12 回路網 $f: X^n \rightarrow C_r^k$ の集合 \mathcal{H}_n は $GF(r^k)$ の上の

階数 r^k の多変数環と同型で, \mathcal{H}_n の性質の元は一意に定まるベクトル基底を $m_i(x_1, x_2, \dots, x_n)$ とすれば次のように展開

$$\text{される; } f(x^n) = \sum_{i=0}^{r^n-1} v_i m_i(x_1, x_2, \dots, x_n) \quad \text{--- (2.7)}$$

$$= \sum_{i=0}^{r^n-1} (v_{i,0} m_i, v_{i,1} m_i, \dots, v_{i,k-1} m_i) \quad \text{--- (2.8)}$$

$$= (x_0, x_1, \dots, x_{k-1})$$

$$\text{但し } v_i = (v_{i,0}, v_{i,1}, \dots, v_{i,k-1}) \in (\mathbb{Z}/(r))^k$$

基本可換群を用いた群関数は図2.2 に示すように各端子毎の関数の表現を与え、 x_i は i 端子の出力関数も示している。

又回路網では G^k の生成元に対応する k 種のセルが必要である。

更にこの時の基底関数は γ 値論理関数のものと同様である。

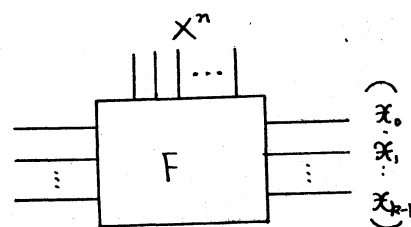


図2.2

これらの (2.4), (2.7) 式は γ 値論理関数の加法展開の一般化であり、これを最小関数表示とよぶ。最小関数表示の項を $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ とするとき長さを $l_n(x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n})$ と定義し、 0 ではない e_i の個数とする。このとき最小関数表示の各項の長さは、セルへの入力数と又係数はその所要個数を示す。従ってこの表示の最大長が n ならば、この回路網は n 変数で合成可能である。故に $(1, k)$ -セルで合成するには何らかの他の方法が必要である。

例題 2. 次の真理値表表示された回路網 $f: X^n \rightarrow G^2$ を最小関数表示せよ。

$$\begin{aligned} F = & (0, 1) J_0(x_1) \cdot J_0(x_2) \oplus (2, 0) J_1(x_1) \cdot J_0(x_2) \oplus (1, 1) J_2(x_1) \cdot J_0(x_2) \\ & \oplus (1, 0) J_0(x_1) \cdot J_1(x_2) \oplus (0, 2) J_1(x_1) \cdot J_2(x_2) \oplus (0, 1) J_2(x_1) \cdot J_1(x_2) \\ & \oplus (1, 2) J_0(x_1) \cdot J_2(x_2) \oplus (0, 0) J_1(x_1) \cdot J_2(x_2) \oplus (2, 1) J_2(x_1) \cdot J_2(x_2) \end{aligned}$$

$$J_0 = 1 \oplus 2x^2, \quad J_1 = 2x \oplus 2x^2, \quad J_2 = 2x^2 \oplus x$$

を代入すれば

$$\begin{aligned}
F &= (2x_1, 1 \oplus x_1 \oplus x_1^2) \oplus (2x_1 \oplus x_1^2, 2x_1 \oplus 2) x_2 \\
&\quad \oplus (2x_1 \oplus 1 \oplus x_1^2, 2x_1 \oplus 2x_1^2) x_2^2 \\
&= (2x_1 \oplus 2x_1x_2 \oplus x_1^2x_2 \oplus 2x_1x_2^2 \oplus x_2^2 \oplus x_1^2x_2^2, \\
&\quad 1 \oplus x_1 \oplus x_1^2 \oplus 2x_1x_2 \oplus 2x_2 \oplus 2x_1x_2^2 \oplus 2x_1^2x_2^2)
\end{aligned}$$

x_2	x_1	f_2	f_1	$2x_1, 2x_1x_2, x_1^2x_2, 2x_1x_2^2, x_2^2, x_1^2x_2^2$	$1, x_1, x_1^2, 2x_1x_2, 2x_2, 2x_1x_2^2, 2x_1^2x_2^2$
0	0	0	1	0 0 0 0 0 0	1 0 0 0 0 0
0	1	2	0	2 0 0 0 0 0	1 1 1 0 0 0
0	2	1	1	1 0 0 0 0 0	1 2 1 0 0 0
1	0	1	0	0 0 0 0 1 0	1 0 0 0 2 0
1	1	0	2	2 2 1 2 1 1	1 1 1 2 2 2
1	2	0	1	1 1 1 1 1 1	1 2 1 1 2 1
2	0	1	2	0 0 0 0 1 0	1 0 0 0 1 0
2	1	0	0	2 1 2 2 1 1	1 1 1 1 1 2
2	2	2	1	1 2 2 1 1 1	1 2 1 2 1 1

表 2.1

2.2. 環論的回路網の合成

回路網の表現としての \mathcal{L}_n は r 元環をなし、 \mathcal{L}_n の加法に対しては回路網のカスケーディングが対応し、各項の変数が入力を示すのである。これに対し \mathcal{L}_n には更に乗法が定義されており、 \mathcal{L}_n の元を r -次元ベクトルとみなした時これは \mathbb{Z}_r の空間の一次変換に対応し回路網では一定のセルの配列に相当する。従って非線形変換もその複雑さより考察の対称より除外すれば回路網合成の問題はアフィン変換の概念を用いて解くことができる。又各入力ベクトルの点を指定するだけであるから、本質的には係数の上の一次変換の性質を調べればよい。

ここでは巡回群 C_{r^k} と基本可換群 C_k の群関数としての回路網について論じる。

定理 1.3. r を 2 と異なる素数とすると、 C_{r^k} の生成元 a に対

して作用素 g_i を $g_i \cdot a = g^{-1} a \cdot g = a^i$ とすれば、 i が r の中と異なるとき単位元を単位元に移す自己同型作用素である。

又 Euler 関数を $\phi(r^k)$ とすれば、この自己同型作用素の全体 $A(C_{r^k})$ は $\phi(r^k)$ 又はその約数を位数とする巡回群をなし、

$$\text{ここで} \quad g = \begin{pmatrix} 0 & 1 & 2 & \cdots & r^{k-1} \\ p & i & 2i & \cdots & (r^{k-1})i \end{pmatrix}$$

(証明) $\text{g.c.d.}(i, r^k) = 1$ であるから、 $\exists p, q \in \mathbb{Z}/(r^k)$

$$pi + q \cdot r^k = 1 \quad \therefore \quad pi \equiv 1 \pmod{r^k}. \quad \text{故に } g_i \text{ は自己同型}$$

更に $i^{\phi(r^k)} \equiv 1 \pmod{r^k}$ より $\varphi_i^{\phi(r^k)} \cdot a = a^{\phi(r^k) \cdot i} = a = \varphi_i \cdot a$

$\therefore \varphi_i^{\phi(r^k)} = \varphi_i$ すなわち φ_i は $\phi(r^k)$ 又はその約数と位数とする巡回群を有す。

$$\text{又 } a = \begin{pmatrix} 0 & 1 & 2 & \cdots & r^{k-1} \\ 1 & 2 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ i & i+1 & i+2 & \cdots & i+r^{k-1} \end{pmatrix} \text{ とおくと } \varphi_i \cdot a = g^{-1} \cdot a \cdot g = \begin{pmatrix} g(0), g(1), \dots \\ g(1), g(2), \dots \\ \vdots \\ g(i), g(i+1), \dots \end{pmatrix} = a^i$$

$$\text{かつ } g(0) = 0 \text{ より } g = \begin{pmatrix} 0 & 1 & 2 & \cdots & r^{k-1} \\ 0 & i & 2i & \cdots & (r^{k-1})i \end{pmatrix} \quad (\text{証明終})$$

図2.3 に示されるようにセル入力 x_n の下で $n-1$ 変数関数に作用素 φ_i を用いることを $\varphi_i^{x_n}$ と表わす。これは空間 SL_n では x_n の指定するベクトル成分に作用素 φ_i を施すことを意味する。真理値表での作用素の働きを表2.2に示す。右点は作用素の有無によって

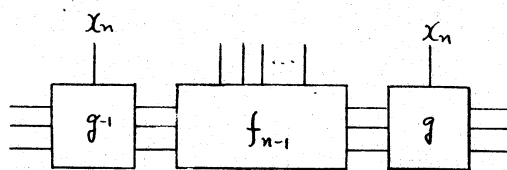


図 2.3

$$i J_e(x_n) \cdot f_{n-1} \text{ 又は } J_e(x_n) f_{n-1}$$

とあり

$$\varphi_i^{x_n} f_{n-1} = J_0(x_n) \cdot f_{n-1} \oplus i J_1(x_n) \cdot f_{n-1}$$

$$\oplus \cdots \oplus i J_{r-1}(x_n) \cdot f_{n-1}$$

と変形される。一般に任意の n 変数関数 f が与えられるとき、その最小関数表示より $n-1$

x_n	$\varphi_i^{x_n} f_{n-1}$	
0	$e \ a_0 \ e$	$J_0(x_n) \cdot f_{n-1}$
	$e \ a_1 \ e$	
	\vdots	
	$e \ a_{r-1} \ e$	
1	$g^{-1} \ a_0 \ g$	$i \cdot J_1(x_n) \cdot f_{n-1}$
	$g^{-1} \ a_1 \ g$	
	\vdots	
	$g^{-1} \ a_{r-1} \ g$	
\vdots	\vdots	
$r-1$	$g^{-1} \ a_0 \ g$	$i \cdot J_{r-1}(x_n) \cdot f_{n-1}$
	$g^{-1} \ a_1 \ g$	
	\vdots	
	$g^{-1} \ a_{r-1} \ g$	

表 2.2

変数関数がある手順で求まれば、この作用素の概念を用いて合成できる。

即ち r 種の $n-1$ 変数関数を $f_{n-1}^0, f_{n-1}^1, \dots, f_{n-1}^{r-1}$ とおくと

$$\begin{cases} \phi_i^{x_n} \cdot f_{n-1}^0 = (\alpha_0 J_0 \oplus \alpha_1 J_1 \oplus \dots \oplus \alpha_{r-1} J_{r-1}) \cdot f_{n-1}^0 \\ \phi_i^{x_n} \cdot f_{n-1}^1 = (\beta_0 J_0 \oplus \beta_1 J_1 \oplus \dots \oplus \beta_{r-1} J_{r-1}) \cdot f_{n-1}^1 \\ \vdots \\ \phi_i^{x_n} \cdot f_{n-1}^{r-1} = (\gamma_0 J_0 \oplus \gamma_1 J_1 \oplus \dots \oplus \gamma_{r-1} J_{r-1}) \cdot f_{n-1}^{r-1} \end{cases} \quad (2.9)$$

各基底関数を代入すると次の連立方程式が求む標準方程式となる。

$$\begin{cases} (\text{定数項}) = (p_0 f_{n-1}^0 \oplus p_1 f_{n-1}^1 \oplus \dots \oplus p_{r-1} f_{n-1}^{r-1}) \\ (x_n \text{ の項 }) = (q_0 f_{n-1}^0 \oplus q_1 f_{n-1}^1 \oplus \dots \oplus q_{r-1} f_{n-1}^{r-1}) \\ \vdots \\ (x_n^{r-1} \text{ の項 }) = (r_0 f_{n-1}^0 \oplus r_1 f_{n-1}^1 \oplus \dots \oplus r_{r-1} f_{n-1}^{r-1}) \end{cases} \quad (2.10)$$

故に各 $n-1$ 変数関数がこれより一意的に求まるには各作用素 $\phi_i^{x_n}$ が独立であればよい。これらを満す作用素は種々あるが計算の簡単さと能率を考えて次の作用素を用いる。

$$\phi_i^x = \phi_j, \quad \phi_i^x \cdot a = \begin{cases} g^{-1} \cdot a \cdot g & \text{if } x=j \\ e \cdot a \cdot e & \text{if } x \neq j \end{cases} \quad (2.11)$$

これを用いた一回路網構成を図2.4に示す。

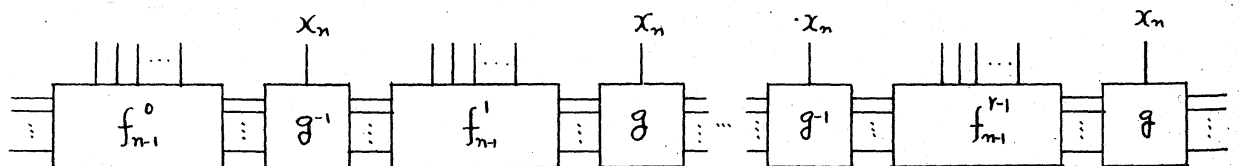


図2.4

補題 2. (i) r は任意の素数とすると $(i-1)^{r-1} \equiv 1 \pmod{r}$

$$(ii) a \equiv 1 \pmod{r} \Rightarrow \gcd(a, r^k) = 1$$

$$(iii) \gcd(a, r^k) = 1 \Rightarrow \exists p \in \mathbb{Z}/(r^k), \quad \frac{1}{a} = p$$

$$(\text{証明}) (i) (i-1)^{r-1} = \frac{(i-1)^r}{(i-1)} = \frac{i^r - 1}{(i-1)} = \frac{i \cdot i^{r-1} - 1}{i-1} = \frac{i-1}{i-1} = 1$$

$$(ii) a \equiv 1 \pmod{r} \Rightarrow a = dr + 1 \text{ とおく } \Rightarrow \gcd(a, r^k) = \gcd(dr+1, r^k) = 1$$

$$(iii) \gcd(a, r^k) = 1 \Rightarrow \exists p, q \in \mathbb{Z}/(r^k), \quad ap + r^k q = 1$$

$$\therefore ap \equiv 1 \pmod{r^k} \text{ すなわち } \frac{1}{a} \equiv \frac{ap}{a} \equiv p \pmod{r^k} \quad (\text{証明終})$$

定理 14. k 出力回路網 $f: X^n \rightarrow C_{r^k}$ は $2r-1$ 種の $(1, k)$ -セルを

用いて常に合成可能で、所要セル数は

$$L_n \leq (r^{k+1} - r + 2) \cdot r^{n-1} - 2 \quad (r \geq 3)$$

(証明) 表 2.3 の作用素と図 2.4

の構成法を用いる。この作用素

が独立であることを示せばよい。

~。

$$\alpha = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & i & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & i \end{vmatrix} = (i-1)^{r-1}$$

x	${}^0\phi_i^x$	${}^1\phi_i^x$	\dots	${}^{r-1}\phi_i^x$
0	1	1		1
1	1	i		1
2	1	1	\dots	1
\vdots	\vdots	\vdots		\vdots
$r-1$	1	1		i

表 2.3

補題より $\alpha = (i-1)^{r-1} \not\equiv 0 \pmod{r^k}$ 故に一次独立である。かつ $\mathbb{Z}/(r^k)$

の閉じた系で解ける。

所要セル数は $L_n = r \cdot L_{n-1} + 2(r-1)$

$$= r^2 L_{n-2} + 2r(r-1) + 2(r-1)$$

$$= \dots = \gamma^{n-1} L_1 + 2 \cdot \gamma^{n-1} - 2 = (L_1 + 2) \cdot \gamma^{n-1} - 2$$

$$L_1 \leq \gamma(\gamma^k - 1) \text{ より } L_n \leq (\gamma^{k+1} - \gamma + 2) \cdot \gamma^{n-1} - 2 \quad (\text{証明終})$$

系.1. γ を 2 と異なる任意の素数とすると、任意の回路網 $f: X^n \rightarrow G$

は (1,1)-セルのカスケードで合成することが出来る。所要セル数

$$\text{は } L_n \leq (\gamma^2 - \gamma + 2) \cdot \gamma^{n-1} - 2$$

同様に基本可換群 G^k の自己同型作用素を T で表わし、 χ の制御

の下での成分の外に変換 T をもつ作用素を T_i^x と書く。

これを表 2.4 に示す。

各自己同型作用素は $Z(r)$ の

元と成分とする $k \times k$ の行列

で表わすことが出来る。

I_k は $k \times k$ の単位行列とする。

χ	T_0^x	T_1^x	\dots	T_{r-1}^x
0	I_k	I_k		I_k
1	I_k	T		I_k
2	I_k	I_k	\dots	I_k
\vdots	\vdots	\vdots		\vdots
$r-1$	I_k	I_k		T

表 2.4

γ 個の $(n-1)$ -変数関数 を $F_{n-1}^0, F_{n-1}^1, \dots, F_{n-1}^{r-1}$ とする。

$$\begin{cases} T_0^{\chi_n} \cdot F_{n-1}^0 = J_0 \cdot F_{n-1}^0 \oplus J_1 \cdot F_{n-1}^0 \oplus \dots \oplus J_{r-1} \cdot F_{n-1}^0 \\ T_1^{\chi_n} \cdot F_{n-1}^1 = J_0 \cdot F_{n-1}^1 \oplus J_1 (F_{n-1}^1 \cdot T) \oplus \dots \oplus J_{r-1} \cdot F_{n-1}^1 \\ \vdots \\ T_{r-1}^{\chi_n} \cdot F_{n-1}^{r-1} = J_0 \cdot F_{n-1}^{r-1} \oplus J_1 \cdot F_{n-1}^{r-1} \oplus \dots \oplus J_{r-1} (F_{n-1}^{r-1} \cdot T) \end{cases} \quad \text{--- (2.12)}$$

故に図 2.4 の構成法を用いれば

$$\begin{aligned} F_n &= T_0^{\chi_n} \cdot F_{n-1}^0 \oplus T_1^{\chi_n} \cdot F_{n-1}^1 \oplus \dots \oplus T_{r-1}^{\chi_n} \cdot F_{n-1}^{r-1} \\ &= J_0 (F_{n-1}^0 \oplus F_{n-1}^1 \oplus \dots \oplus F_{n-1}^{r-1}) \oplus J_1 (F_{n-1}^0 \oplus F_{n-1}^1 \cdot T \oplus \dots \oplus F_{n-1}^{r-1}) \oplus \dots \end{aligned}$$

$$\dots \oplus J_{r-1} (F_{m-1}^0 \oplus F_{m-1}^1 \oplus \dots \oplus F_{m-1}^{r-1} \cdot T) \quad \text{--- (2.13)}$$

J_0, J_1, \dots, J_{r-1} を代入すれば

$$\begin{cases} M_{0,0} F_{m-1}^0 \oplus M_{0,1} F_{m-1}^1 \oplus \dots \oplus M_{0,r-1} F_{m-1}^{r-1} & = (\text{定数項}) \\ M_{1,0} F_{m-1}^0 \oplus M_{1,1} F_{m-1}^1 \oplus \dots \oplus M_{1,r-1} F_{m-1}^{r-1} & = (x \text{ の項}) \\ \vdots & \\ M_{r-1,0} F_{m-1}^0 \oplus M_{r-1,1} F_{m-1}^1 \oplus \dots \oplus M_{r-1,r-1} F_{m-1}^{r-1} & = (x^{r-1} \text{ の項}) \end{cases} \quad \text{--- (2.14)}$$

が求まる。この式を基本可換群の標準方程式とよぶ。ここで M_{ij} は $k \times k$ の行列で自己同型作用素 T と単位行列 I_k との組み合わせよりなる。従って体をつくっている。次に表2.4の作用素が一次独立な k の条件を求める。

$$\Sigma = \begin{vmatrix} I_k & I_k & \dots & I_k \\ I_k & T & \dots & I_k \\ \vdots & \vdots & \ddots & \vdots \\ I_k & I_k & \dots & T \end{vmatrix} = | (T \oplus I_k)^{r-1} | \neq 0 \pmod{r}$$

が成り立てばよから、 T は固有値1を持つ自己同型作用素であればよい。

$GF(r)$ の次の k 次方程式を

$$f(x) = x^k + \alpha_{k-1} x^{k-1} + \dots + \alpha_1 x + \alpha_0$$

とすると、この随伴行列 (Companion matrix) はベクトル空間の線形変換に対応し、自明で自己同型作用素を示している。

$$T_c = \begin{vmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ & & \vdots & & & \\ 0 & 0 & \cdots & 0 & 1 \\ -\alpha_0 & -\alpha_1 & \cdots & -\alpha_{k-1} & -\alpha_k \end{vmatrix}$$

定理 15. k 出力回路網 $f: X^n \rightarrow G_r^k$ は $(2r+k-2)$ 種の $(1, k)$ -セルを用いて常に合成可能であり、所要セル数は

$$L_n \leq k(r^{n+1} - r^n) + 2 \cdot r^{n-1} - 2$$

(証明) 半前は明らか。所要セル数は図 2.4 と同じ構成を用いる。
 は $L_n = (L_1 + 2)r^{n-1} - 2$.

$$\begin{aligned} L_1 &\leq (r-1) \cdot r \cdot k & \therefore L_n &\leq \{k(r^2 - r) + 2\} \cdot r^{n-1} - 2 \\ & & &= k(r^{n+1} - r^n) + 2 \cdot r^{n-1} - 2 \end{aligned}$$

又セルの種類は G_r^k の生成元 k 個、作用セル $2r-2$ 個より

$(2r+k-2)$ -種のセルが必要。

(証明終)

2.3. 三値論理関数とその合成

実際の回路網の合成を考えると、多値論理関数のうちでも、三値論理関数が重要である。又三値の場合が状態に冗長度ほしにカスケード合成できる最小の状態数である。三値論理関数の合成について例題を中心に考察する。

補題 3. 位数3の巡回群 G の単位元を単位元に移す自己同型

作用素で自明なもの $g \cdot a = g^2 a \cdot g = a^2$ だけで、 $g^3 = 1$

定理 16. 任意の三値一出力回路網は三種の (1,1)-セルを用いて

所要セル数 $L_n \leq 8 \cdot 3^{n-1} - 2$ で合成可能である。

(証明略)

例題 3. 次の与えられた関数を合成せよ。

x	y	f	f_0				f_1				f_2			
			x	x	x	2	x	2	y^2	$2y$	x	y^2	x	y^2
0	0	1	e	e	e	a^2	e	a^2	e	e	e	e	e	e
0	1	2	e	e	e	a^2	e	a^2	a	a^2	e	a	e	e
0	2	1	e	e	e	a^2	e	a^2	a	a	e	a	e	e
1	0	0	g^{-1}	e	g^{-1}	a^2	g	a^2	e	e	e	e	g	g
1	1	2	g^{-1}	e	g^{-1}	a^2	g	a^2	a	a^2	e	a	g	g
1	2	0	g^{-1}	e	g^{-1}	a^2	g	a^2	a	a	e	a	g	g
2	0	1	g^{-1}	g^{-1}	e	a^2	e	a^2	e	e	g	e	e	e
2	1	0	g^{-1}	g^{-1}	e	a^2	e	a^2	a	a^2	g	a	e	e
2	2	2	g^{-1}	g^{-1}	e	a^2	e	a^2	a	a	g	a	e	e

表 2.5

真理値表表示を展開する

$$f = x^2 \oplus x^2 y \oplus xy \oplus 2xy^2 \oplus x \oplus 2y^2 \oplus 2y \oplus 1$$

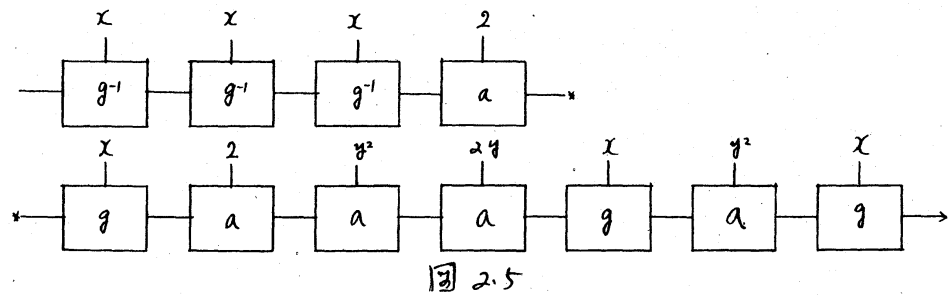
(i) 図2.5 のような構成法を用いると

$$f = [\{ (J_0 \oplus 2J_1 \oplus J_2) f_0 \oplus f_1 \} (J_0 \oplus J_1 \oplus 2J_2) \oplus f_2] (J_0 \oplus 2J_1 \oplus J_2)$$

より標準方程式は

$$\begin{cases} (\text{定数項}) = f_0 \oplus f_1 \oplus f_2 = 2\gamma^2 \oplus 2\gamma \oplus 1 \\ (x \text{ の項}) = 2f_1 = \gamma \oplus 2\gamma^2 \oplus 1 \\ (x^2 \text{ の項}) = 2f_1 \oplus f_2 = \gamma \oplus 1 \end{cases}$$

$$\text{故に } f_0 = 2, \quad f_1 = \gamma^2 \oplus 2\gamma \oplus 2, \quad f_2 = \gamma^2$$



(ii) 図2.6 の構成法を用いる。

$$f = (J_0 \oplus J_1 \oplus J_2) f_0 \oplus (J_0 \oplus 2J_1 \oplus J_2) f_1 \oplus (J_0 \oplus J_1 \oplus 2J_2) f_2$$

標準方程式は

$$\begin{cases} (\text{定数項}) = f_0 \oplus f_1 \oplus f_2 = 2\gamma^2 \oplus 2\gamma \oplus 1 \\ (x \text{ の項}) = 2f_1 \oplus f_2 = 2\gamma^2 \oplus \gamma \oplus 1 \\ (x^2 \text{ の項}) = 2f_1 \oplus 2f_2 = \gamma \oplus 1 \end{cases}$$

$$\text{故に } f_0 = 2\gamma^2 \oplus 2, \quad f_1 = 2\gamma^2 \oplus 2\gamma \oplus 2, \quad f_2 = \gamma^2$$

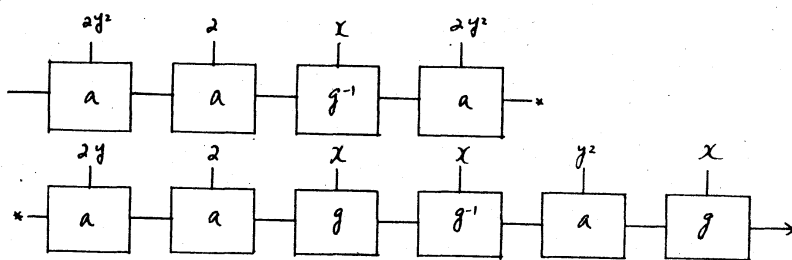


図2.6

次に多出力回路網の合成についてのべる。まず巡回群 C_{3^k} の

変換回路網は最小関

数表示が $\text{mod } 3^k$ での

演算であるから表2.7

より次の結果を得る。

x	x^2	1	$(3^k-1)x^2$	$(3^k-1)x$	$2x^2$
0	0	1	0	0	0
1	1	1	3^k-1	3^k-1	2
2	1	1	3^k-1	3^k-2	2

表2.7

定理17 回路網 $f: X^n \rightarrow C_{3^k}$ の基底関数は次のように与えられる。

$$\begin{cases} J_0(x) = 1 \oplus (3^k-1)x^2 \\ J_1(x) = (3^k-1)x \oplus 2x^2 \\ J_2(x) = x \oplus (3^k-1)x^2 \end{cases} \quad (2.15)$$

このとき作用素としてはいろいろあるが、二面体群作用素

が 3^k が奇数であるので条件を満たし

$$g_{r^{3^k}} \cdot a = a^{r^{3^k}} = g^{-1} \cdot a \cdot g$$

かつ $g^{-1} = g$ である。

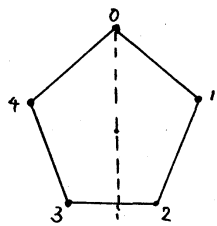


図2.7

定理18 任意の3値k出力回路網は二面体群セルを用いて

3種のセルで常に合成可能。所要セル数は

$$L_n \leq (3^{k+1}-1)3^{n-1}-2$$

(証明略)

基本可換群による合成法も同様に成り立つが、巡回群の場合に比してセルの種類が増え、所要個数が減っている。

例題 4. 次の関数を回路網 $f: X^2 \rightarrow G^3$ として実現せよ。

$x_2 \ x_1$	$f_2 \ f_1$	$x_2(2x_1, 2x_1^2, 2, x_1, 2x_1^2)x_2, x_2(1, 2x_1, 1, 2x_1)x_2, x_2(2, x_1, x_1^2, 1, x_1, 2x_1^2)x_2$
0 0	0 1	e e e a_3^2 e e e e a_1 e a_3 a_3^2 e e a_1^2 e e a_3 e e e
0 1	2 0	e a_1^2 a_1^2 a_3^2 a_3 a_3^2 e e a_1 a_1^2 a_3 a_3^2 e e a_1^2 a_1 a_1 a_3 a_3 a_3^2 e
0 2	1 1	e a_1 a_1^2 a_3^2 a_3^2 a_3^2 e e a_1 a_1 a_3 a_3 e e a_1^2 a_1^2 a_1 a_3 a_3^2 a_3 e
1 0	1 0	g^{-1} e e a_3^2 e e g e a_1 e a_3 e e g^{-1} a_1^2 e e a_3 e e g
1 1	0 2	g^{-1} a_1^2 a_1^2 a_3^2 a_3 a_3^2 g e a_1 a_1^2 a_3 a_3^2 e g^{-1} a_1^2 a_1 a_1 a_3 a_3 a_3^2 g
1 2	0 1	g^{-1} a_1 a_1^2 a_3^2 a_3^2 a_3^2 g e a_1 a_1 a_3 a_3 e g^{-1} a_1^2 a_1^2 a_1 a_3 a_3^2 a_3 g
2 0	1 2	e e e a_3^2 e e e g^{-1} a_1 e a_3 e g g^{-1} a_1^2 e e a_3 e e g
2 1	0 0	e a_1^2 a_1^2 a_3^2 a_3 a_3^2 e g^{-1} a_1 a_1^2 a_3 a_3^2 g g^{-1} a_1^2 a_1 a_1 a_3 a_3 a_3^2 g
2 2	2 1	e a_1 a_1^2 a_3^2 a_3^2 a_3^2 e g^{-1} a_1 a_1 a_3 a_3 g g^{-1} a_1^2 a_1^2 a_1 a_3 a_3^2 a_3 g

表 2.6

表 2.6. 図 2.7 に示すような構成を用いると標準方程式は

$$\begin{cases} F_{n-1}^1 \oplus F_{n-1}^2 \oplus F_{n-1}^3 = (\text{定数}) \\ F_{n-1}^1(I_k \oplus 2T) \oplus F_{n-1}^2(2I_k \oplus T) = (x \text{ の項}) \\ F_{n-1}^1(I_k \oplus 2T) \oplus F_{n-1}^2(I_k \oplus 2T) \oplus F_{n-1}^3(2I_k \oplus T) = (x^2 \text{ の項}) \end{cases}$$

として求まる。

すなわち真理値表表示を展開すると

$$F = (2x_1, 1 \oplus x_1 \oplus x_1^2) \oplus (2x_1 \oplus x_1^2, 2x_1 \oplus 2) x_2 \\ \oplus (2x_1 \oplus x_1^2, 2x_1 \oplus 2x_1^2) x_2^2$$

$$\text{故に} \begin{cases} F^1 \oplus F^2 \oplus F^3 = (2x_1, 1 \oplus x_1 \oplus x_1^2) = g_1 \\ F^1(I_k \oplus 2T) \oplus F^2(2I_k \oplus T) = (2x_1 \oplus x_1^2, 2x_1 \oplus 2) = g_2 \\ F^1(I_k \oplus 2T) \oplus F^2(I_k \oplus 2T) \oplus F^3(2I_k \oplus T) = (2x_1 \oplus 1 \oplus x_1^2, 2x_1 \oplus 2x_1^2) = g_3 \end{cases}$$

$$\therefore \text{より} \quad \begin{cases} F^1 = g_1 \oplus (g_3 \oplus 2g_2)(T \oplus 2I_k)^{-1} \\ F^2 = g_1 \oplus 2(g_2 \oplus g_3)(T \oplus 2I_k)^{-1} \\ F^3 = g_1 \oplus g_3(T \oplus 2I_k)^{-1} \end{cases}$$

自己同型作用素として

$$T = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \quad T \cong \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 2 & 5 & 7 & 1 & 4 & 7 \end{pmatrix}$$

$$= (1326)(4578)$$

をとると

$$\begin{cases} F^1 = (2\chi_1 \oplus 2\chi_1^2, 2 \oplus 2\chi_1^2) \\ F^2 = (1 \oplus 2\chi_1, 1 \oplus 2\chi_1) \\ F^3 = (2 \oplus \chi_1 \oplus \chi_1^2, 1 \oplus \chi_1 \oplus 2\chi_1^2) \end{cases}$$

故に次の回路網を得る。

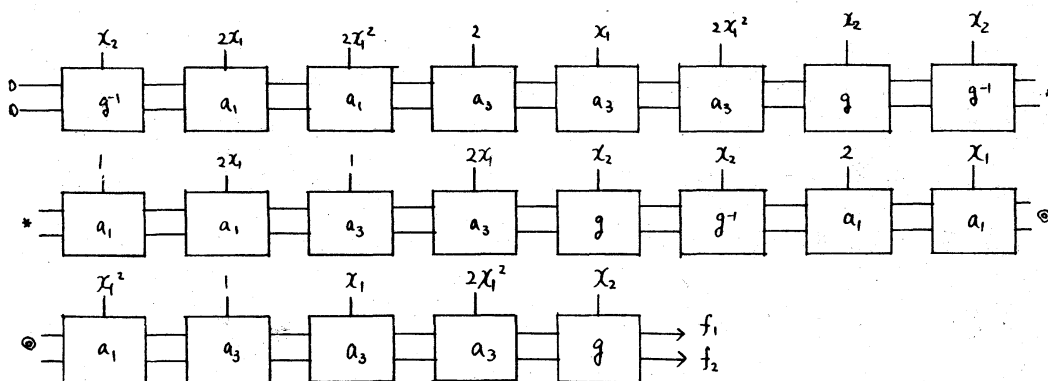


図 2.7

回路網の単純化等を考慮すれば、セルの個数の増加をある程度許しても、セルの種類が少い方が有利なこともある。二値の場合は全ての群セルは一種のもので置き換えることができた。三値について次に述べる。

S_p を p 次の対称群とする, $\forall a, b \in S_p$, $G = \{a, b\}$ とおくと、 $G^{(2)} = \{a^2, ab, ba, b^2\}$, $G^{(i)} = G^{(i-1)} \cdot G$ と定義する。

$$\langle \{G\} \rangle = \{G, G^{(2)}, \dots, G^{(p)}\}$$

を G より生成された巡回群とよび, $G^{(p+r)} = G^{(r)}$ なる r を $\langle \{G\} \rangle$ の周期とよぶ。回路網 $f(x) = (g_1, g_2, g_3)$ がセル $\theta(x) = (a_1, a_2, a_3)$ の l 段のカスケードで実現されるには $G = \{a_1, a_2, a_3\}$ とすると $G^{(l)}$ に g_1, g_2, g_3 が必要である。

定理 19 p 次の対称群 S_p は二種の生成元

$$a_1 = (12) \text{ と } a_2 = (12 \dots p), \text{ 又は } a_3 = (23 \dots p)$$

で生成される。即ち $\langle \{a_1, a_2\} \rangle = \langle \{a_1, a_3\} \rangle = S_p$

(証明) $a_2 = a_1 a_3$ より $\langle \{a_1, a_2\} \rangle = \langle \{a_1, a_3\} \rangle$

従って $\langle \{a_1, a_2\} \rangle = S_p$ を示そう。

$$\forall s \in S_p, \quad s = (i_1, i_2, \dots, i_l) = (i_1, i_2)(i_2, i_3) \dots (i_{l-1}, i_l)$$

かつ $(i_l, i_m) = (i_1, i_l)(i_1, i_m)(i_1, i_l)$ より 任意の l は次の互換の積として書ける

$$(i_1, i_2), (i_1, i_3), \dots, (i_1, i_l)$$

更に $a_3^{-k} (1, r-k+1) = (12) a_3^k$ より

$$(1, r-k+1) = a_3^{-k} (12) a_3^k$$

$$\therefore \langle \{a_1, a_2\} \rangle = S_p \quad (\text{証明終})$$

定理 20. 三値多出力回路網は一種のセルで合成する：ことがで

きる。即ち反復論理回路網で実現できる。

(証明) 入力変数集合 $\{0, 1, 2, x, x^2\}$ に対して

$$\text{セル } \theta \text{ を } \theta(x) = (a_2, a_1, a_2^x), (x, p) = 1 \text{ とおく}$$

$$(1) \theta(0) = (a_2, a_2, a_2) \quad (2) \theta(1) = (a_1, a_1, a_1)$$

$$(3) \theta(2) = (a_2^2, a_2^2, a_2^2) \quad (4) \theta(x) = (a_2, a_1, a_2^x)$$

$$(5) \theta(x^2) = (a_2, a_1, a_1)$$

a_1, a_2 の位数はそれぞれ 2 と $p \cdot 3^k$ である。特に $k=2$ とする。

$$(4) \text{ より } (a_2, a_1, a_2^2)^p = (a_2^p, a_1^p, a_2^{2p}) = (e, a_1, e) \quad (6)$$

$$(a_2, a_1, a_2^2)^{p+1} = (a_2, e, a_2^2) \quad (7)$$

$$(5) \text{ より } (a_2, a_1, a_1)^p = (e, a_1, a_1) \quad (8)$$

$$(6), (8) \text{ より } (e, a_1, e) \cdot (e, a_1, a_1) = (e, e, a_1) \quad (9)$$

$$(2), (8) \text{ より } (a_1, a_1, a_1) \cdot (e, a_1, a_1) = (a_1, e, e) \quad (10)$$

$$(5) \text{ より } (a_2, a_1, a_1) \text{ に対して } \exists r_1, r_2, -pr_1 + 2 \cdot r_2 = 1$$

$$\therefore (a_2, a_1, a_1)^{2r_2} = (a_2^{pr_1+1}, e, e) = (a_2, e, e) \quad (11)$$

$$\therefore (7), (11) \text{ より } (a_2, e, e)^{p-1} \cdot (a_2, e, a_2^2) = (e, e, a_2^2) \quad (12)$$

$$(3), (11), (12) \text{ より } (a_2^2, a_2^2, a_2^2) \cdot (a_2, e, e)^{p-2} \cdot (e, e, a_2^2)^{p-1} = (e, a_2^2, e) \quad (13)$$

$$\text{故に } \left\{ \begin{array}{ll} (a_1, e, e) & (a_2, e, e) \\ (e, a_1, e) & (e, a_2^2, e) \\ (e, e, a_1) & (e, e, a_2^2) \end{array} \right\}$$

が求まり, $(2, p) = 1$ より $\exists r_1, r_2, 2r_1 - pr_2 = 1$

$$\therefore (e, a_2^2, e)^{2r_1} = (e, a_2, e).$$

$$\text{同様} \quad (e, e, a_2^2)^{2r_1} = (e, e, a_2)$$

$$\text{故に} \quad \langle \theta(x) = (a_2, a_1, a_2^2) \rangle = S_p \times S_p \times S_p$$

(証明終)

結言. ある種の完備な論理系を定義し, それらの論理系の代数的構造とそれらの性質について述べ, 更に多段論理回路網での合成に関して純代数的に考察した。この多段論理回路網は可換環の上の多え環として表示され, 線形変換の概念を用ゐれば与えられた変数関数の展開式上の変形を見出すことにより, ^(合成)可能であった。その結果任意の多出力回路網は巡回群又は基本可換群セルを用ゐればその作用素セルが存在して合成可能である。ここで述べた性質は回路網合成の可能性の判定のみならず, 論理関数の性質を調べるのにも重要であると思われる。最後にいろいろ討論したばかり研究室の皆様に深謝致します。

文献

- (1) M. H. Stone : Boolean algebras Harvard Uni 1936
- (2) R. L. Herrmann : Selection and Implementation of Ternary
Switching Algebra. Spring Joint Comp. Conf. 1968
- (3) Yoeli : A group-theoretical approach to two-rail
Cascades. IEEE. EC-14. 1965
- (4) Elspas & Stone : Decomposition of group functions and the
synthesis of multi-rail cascades. IEEE. 8-th annual
symp. on Switching & Automata theory 1967
- (5) 原尾 鈴木 野口 大泉 : 多出力多段論理回路網に関する
基礎的考察. オートマタ・インフォメーション研究会資料 1968
- (6) " : 多段論理回路網の多変数表示と
の合成法. 電子通信学会全国大会 1968
- (7) " : A fundamental consideration on the
multi-staged logical network. The 2nd Hawaii International
Conference on system sciences 1969
- (8) 鈴木 野口 大泉 : 多段論理回路網の構造に関する一考察
電通学会誌 vol. 51-C, No. 7. 1968
- (9) 原尾 鈴木 野口 大泉 : 多出力多段論理回路網の合成
電通学会誌 vol 52-C, No. 9. 1969